AD-A030693

ON COMBINING PSEUDORANDOM NUMBER GENERATORS

by

Mark Brown and Herbert Solomon

Technical Report No. 233
July 15, 1976

Prepared under Contract N00014-76-C-0475
(NR-042-267)
Office of Naval Research

Herbert Solomon, Project Director

DEPARTMENT OF STATISTICS
STANFORD UNIVERSITY
STANFORD, CALIFORNIA

Introduction

Many methods have been proposed, tested and employed for generating pseudorandom numbers ([2], [3], [4], [5], [7], [9], [10], [12], [13]). The goal is to produce strings of numbers which behave like independent uniform $[0,1]$ random variables. The generators yield integers in the set $\{0,\ldots,m-1\}$ which are then transformed to $[0,1]$ by division by m.

Suppose that $X_1, X_2, \ldots$ and $Y_1, Y_2, \ldots$ are strings of numbers in $\{0,\ldots,m-1\}$ generated by two separate generators. Assume that the two strings are independent. Define a new string of numbers $Z_1, Z_2, \ldots$ by $Z_i = X_i + Y_i \pmod{m}$. For any k and corresponding $i_1,\ldots,i_k$ define $\underline{X} = (X_{i_1},\ldots,X_{i_k})$, $\underline{Y} = (Y_{i_1},\ldots,Y_{i_k})$, $\underline{Z} = (Z_{i_1},\ldots,Z_{i_k})$. Let r be the distribution of k independent random variables uniformly distributed on $\{0,\ldots,m-1\}$. We consider several natural measures of distance between multivariate distribution with components in $\{0,\ldots,m-1\}$ and show under these distances that $Z_{i_1},\ldots,Z_{i_k}$ has a distribution closer to r than either $X_{i_1},\ldots,X_{i_k}$ or $Y_{i_1},\ldots,Y_{i_k}$ for all k, $i_1,\ldots,i_k$.

In applying our results to pseudorandom number generation, two points need careful scrutiny. First, we assume that the two strings, X and Y, are independent. Secondly, X, Y and Z are deterministic, even though they are being constructed to look random. This creates a problem in the interpretation of Lemma 1 and in the interpretation of independence. We certainly do not claim that our results prove that addition mod (m) of separately generated sequences improves pseudorandom number generation. We only assert that this conclusion is <u>suggested</u> and warrants further study.

The technique of combining strings by addition mod m is also mentioned in Knuth ([5], p. 30). An exercise at the end of the section (p. 33) shows that if the periods of $\underline{X}$ and $\underline{Y}$ are λ_1, λ_2 with λ_1 and λ_2 relatively prime, then the period of $\underline{Z}$ is $\lambda_1\lambda_2$. This implies that we should choose the periods of the separate generators to be relatively prime.

Random number generators are generally studied by statistical tests on the output, and by mathematical analysis of the period. We hope that the methods employed here will provide another approach to analyzing pseudorandom number generators.

Results

Suppose that $\underline{X} = (X_1,\ldots,X_k)$ and $\underline{Y} = (Y_1,\ldots,Y_k)$ are independent random vectors with $\Pr(X_1=j_1,\ X_2=j_2,\ \ldots,\ X_k=j_k) = p(j_1,\ldots,j_k)$, $\Pr(Y_1=\ell_1,\ Y_2=\ell_2,\ \ldots,\ Y_k=\ell_k) = q(\ell_1,\ldots,\ell_k)$; each component assumes values in $\{0,\ldots,m-1\}$. Define $Z = (Z_1,\ldots,Z_k)$ with $Z_i = X_i + Y_i$ (mod m), and $\Pr(Z_1=m_1,\ \ldots,\ Z_k=m_k) = s(m_1,\ldots,m_k)$. As measures of departure of a distribution b on $\overset{k}{\underset{i=1}{X}} \{0,\ldots,m-1\}_i$, from r the distribution of k independent uniforms on $\{0,\ldots,m-1\}$, we use:

$$\text{(i)}\quad \|b-r\|_\alpha = \sum_{(j_1,\ldots,j_k)} \left|b(j_1,\ldots,j_k) - \frac{1}{m^k}\right|^\alpha , \quad 1 \le \alpha < \infty ,$$

$$\text{(ii)}\quad \|b-r\|_\infty = \max_{(j_1,\ldots,j_k)} \left|b(j_1,\ldots,j_k) - \frac{1}{m^k}\right| ,$$

$$\text{(iii)}\quad \Pi(b,r) = \sum_{(j_1,\ldots,j_k)} b(j_1,\ldots,j_k) \log(m^k b(j_1,\ldots,j_k)) .$$

Quantity (iii) is the mean information in favor of b against the distribution r (see Kullback [6], p. 5); $\Pi(b,r)$ achieves a minimum of 0 at $b = r$ and is otherwise positive.

Lemma 1: For $1 \le \alpha \le \infty$, $\|s - r\|_\alpha \le \min(\|p-r\|_\alpha, \|q-r\|_\alpha)$, and $\Pi(s,r) \le \min(\Pi(p,r),\Pi(q,r))$.

Proof of Lemma 1: We rely heavily on the technique of majorization ([1], [8], [11]). Firstly, adding $\underline{Y}$ to an independent random variable $\underline{X}$ is equivalent to making a transition in the Markov chain with transition matrix $P_{(j_1,\ldots,j_k),(\ell_1,\ldots,\ell_k)} = r(\ell_1 - j_1 (\text{mod } m),\ \ell_2 - j_2 (\text{mod } m),\ \ldots,\ \ell_k - j_k (\text{mod } m))$.

$$\text{Now} \sum_{(j_1,\ldots,j_k)} P_{(j_1,\ldots,j_k),(\ell_1,\ldots,\ell_k)} = \sum_{(m_1,\ldots,m_k)} r(m_1,\ldots,m_k) = 1$$

($(m_1,\ldots,m_k)$ ranges through the m^k sample points achieving each exactly once). Therefore P is doubly stochastic. Next, $s = pP$ with P doubly stochastic and it thus follows from a theorem of Karamata ([1], pg. 31) that s is majorized by p. By definition this means that if s and p are rearranged so that $s_{(1)} \ge s_{(2)} \ge \cdots \ge s_{(m^k)}$ and $p_{(1)} \ge p_{(2)} \ge \cdots \ge p_{(m^k)}$, then $\sum_{i=1}^{j} s_{(i)} \le \sum_{i=1}^{j} p_{(i)}$ for $j = 1,2,\ldots,m^k-1$, and $\sum_{i=1}^{m^k} s_{(i)} = \sum_{i=1}^{m^k} p_{(i)}$.

It follows from the definition of majorization that if s is majorized by p then $s - \frac{1}{m^k}$ is majorized by $p - \frac{1}{m^k}$. For $1 \le \alpha \le \infty$, $|x|^\alpha$ is continuous and convex; it then follows from [1], p. 30, that $\|s - r\|_\alpha \le \|p - r\|_\alpha$.

From the definition of majorization, we know that $s_{(1)} \leq p_{(1)}$ while $s_{(m^k)} \geq p_{(m^k)}$. Therefore

$$\|s - r\|_\infty = \max(s_{(1)} - \frac{1}{m^k}, \frac{1}{m^k} - s_{(m^k)}) \leq \max(p_{(1)} - \frac{1}{m^k}, \frac{1}{m^k} - p_{(m^k)}) = \|p - r\|_\infty .$$

Finally, the function $F(x_1, \ldots, x_{m^k}) = \sum_{i=1}^{m^k} x_i \log(m^k x_i)$ satisfies $(x_i - x_j)\left(\frac{\partial F}{\partial x_i} - \frac{\partial F}{\partial x_j}\right) = (x_i - x_j) \log \frac{x_i}{x_j} \geq 0$ for $x_i \geq x_j$. It then follows from a theorem of Ostrowski ([1], p. 32) and the majorization of s by p that $\Pi(s,r) \leq \Pi(p,r)$.

By reversing the roles of X and Y it follows that $\|s - r\|_\alpha \leq \|q - r\|_\alpha$, $1 \leq \alpha \leq \infty$, and $\Pi(s,r) \leq \Pi(q,r)$. This concludes the proof.

Undoubtedly our result will hold for many other metrics.

If we take an independent sequence of random vectors $\underline{X}_1, \ldots, \underline{X}_n, \ldots$ and form partial sums (mod m), $\underline{Z}_n = \sum_{i=1}^{n} \underline{X}_i$ (mod m), $n = 1,2,\ldots$, we will, under weak conditions, converge at a geometric rate to r. This follows from standard Markov chain analysis.

More specifically, assume that

$$\min_{(j_1, \ldots, j_k)} \Pr(\underline{X}_{(i),1} = j_1, \ldots, X_{(i),k} = j_k) = \Delta_i \geq \Delta > 0$$

for all i. Then, letting s_n denote the distribution of $\underline{Z}_n$, it follows that

$$\max_{(j_1, \ldots, j_k)} s_n(j_1, \ldots, j_k) - \min_{(j_1, \ldots, j_k)} s_n(j_1, \ldots, j_k) \leq \sum_{i=1}^{n} (1 - m^k \Delta_i)$$

$$\leq (1 - m^k \Delta)^n \to 0$$

as $n \to \infty$. For interpreting this result, note that

$$\max_{(j_1,\ldots,j_k)} s_n(j_1,\ldots,j_k) - \min_{(j_1,\ldots,j_k)} s_n(j_1,\ldots,j_k)$$

$$= \max_{(j_1,\ldots,j_k),(\ell_1,\ldots,\ell_k)} \left| s_n(j_1,\ldots,j_k) - s_n(\ell_1,\ldots,\ell_k) \right|$$

$$\geq \max_{(j_1,\ldots,j_k)} \left| s_n(j_1,\ldots,j_k) - \frac{1}{m^k} \right| .$$

The proof is simple. Let $M_n = \max_{(j_1,\ldots,j_k)} s_n(j_1,\ldots,j_k)$ and $m_n = \min_{(j_1,\ldots,j_k)} s_n(j_1,\ldots,j_k)$. Then

$$M_n \leq M_{n-1}(1 - (m^k-1)\Delta_n) + \Delta_n(1 - M_{n-1}) = M_{n-1}(1 - m^k\Delta_n) + \Delta_n ,$$

while

$$m_n \geq m_{n-1}(1 - (m^k-1)\Delta_n) + \Delta_n(1 - m_{n-1}) = m_{n-1}(1 - m^k\Delta_n) + \Delta_n .$$

Thus $M_n - m_n \leq (M_{n-1} - m_{n-1})(1 - m^k\Delta_n)$. Repeated use of this argument gives

$$(M_n - m_n) \leq (M_1 - m_1) \prod_{i=2}^{n} (1 - m^k\Delta_i) \leq \sum_{i=1}^{n} (1 - m^k\Delta_i) \leq (1 - m^k\Delta)^n .$$

Under the weaker condition $\sum_{i=1}^{\infty} \Delta_i = \infty$, we still get $\lim_{n\to\infty} (M_n - m_n) = 0$, although not necessarily convergence at a geometric rate. The condition $\sum_{i=1}^{\infty} \Delta_i = \infty$ is sufficient but not necessary for

convergence of $M_n - m_n$ to 0. For example, if any one $\Delta_i = \frac{1}{m^k}$ (equivalently if any one $\underline{X}_{(i)}$ has distribution r) then the distribution of $\underline{Z}_n$ is r for all $n \geq i$.

Acknowledgment

We would like to thank Professor Donald Knuth of Stanford University for his comments in connection with an earlier version of this paper.

References

[1] Beckenbach, Edwin F. and Bellman, Richard (1965), Inequalities, Springer-Verlag, New York.

[2] Coveyou, R. R. (1960), "Seriel correlation in the generator of pseudorandom numbers," J. Assoc. Comp., 72-74.

[3] Greenberger, M. (1961), "On a priori determination of serial correlation in computer generated random numbers," Math. of Comp., 15, 383-89.

[4] Hull, T. E. and Dobell, A. R. (1962), "Random number generators," SIAM Review, 4, 230-254.

[5] Knuth, Donald E. (1969), The Art of Computer Programming, Volume II; Seminumerical Algorithms, Addison-Wesley, Reading, Massachusetts.

[6] Kullback, S. (1959), Information Theory and Statistics, John Wiley, New York.

[7] Maclarin, M. D. and Marsaglia, G. (1965), "Uniform random number generators," J. Assoc. Comp. Mach., 12, 83-89.

[8] Marshall, A. W., Olkin, I., and Proschan, F. (1967), Monotonicity of ratios of means and other applications of majorization, in Inequalities, ed. by O. Shisha, Academic Press, New York, 170-190.

[9] Meyer, H. A., editor (1956), "Symposium on Monte Carlo Methods," John Wiley and Sons, New York.

[10] Monte Carlo Methods (1951), N.B.S. Applied Mathematics Series No. 12, U.S. Government Printing Office.

[11] Proschan, F. (1975), "Applications of majorization and Schur functions in reliability and life testing," in Reliability and Fault Tree Analysis, ed. by R. E. Barlow, Jerry B. Fussel and Nozer D. Singpurwalla, SIAM, Philadelphia.

[12] Rotenberg, A. (1960), "A new pseudorandom number generator," J. Assoc. Comp. Mach., 7, 75-77.

[13] Strawderman, W. E. (1971), "Generation and testing of pseudorandom numbers," Technical Report No. 171, Department of Statistics, Stanford University.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE

READ INSTRUCTIONS BEFORE COMPLETING FORM

1. REPORT NUMBER: 233
2. GOVT ACCESSION NO.
3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle): (6) On Combining Pseudorandom Number Generators.
5. TYPE OF REPORT & PERIOD COVERED: (9) Technical ~~Report~~,
6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s): (10) Mark/Brown [redacted] Herbert/Solomon
8. CONTRACT OR GRANT NUMBER(s): (15) N00014-76-C-0475
9. PERFORMING ORGANIZATION NAME AND ADDRESS: Department of Statistics, Stanford University, Stanford, Calif. 94305
10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS: (16) (NR-042-267)
11. CONTROLLING OFFICE NAME AND ADDRESS: Office of Naval Research, Statistics & Probability Program Code 436, Arlington, Virginia 22217
12. REPORT DATE: (11) 15 Jul[redacted]76
13. NUMBER OF PAGES
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office): (12) 11p.
15. SECURITY CLASS. (of this report): Unclassified
15a. DECLASSIFICATION/DOWNGRADING SCHEDULE
16. DISTRIBUTION STATEMENT (of this Report): Approved for Public Release; Distribution Unlimited (14) TR-233
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)
18. SUPPLEMENTARY NOTES
19. KEY WORDS (Continue on reverse side if necessary and identify by block number): random number generators, majorization, stochastic matrices
20. ABSTRACT (Continue on reverse side if necessary and identify by block number): (see reverse side)

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-014-6601

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

332 580

4B

20. Let $\underline{X} = (X_1,\ldots,X_n)$ and $\underline{Y} = (Y_1,\ldots,Y_n)$ be independent random vectors whose components take values in $\{0,1,\ldots,m-1\}$. Let r be the joint distribution of n independent random variables uniformly distributed on $\{0,1,\ldots,m-1\}$. We show that the distribution of $\underline{Z} = \underline{X} + \underline{Y}$ (mod m) is closer to r, in several metrics, than is either the distribution of $\underline{X}$ or of $\underline{Y}$. The principle suggested by this result is that combining strings of pseudorandom numbers, generated by different generators, by addition mod m, will result in a string more random than any of the separate strings.